36. The universal-signature-object viewer of claim 35 wherein the verification means verifies the digital signature against an archived copy of the digital signature obtained from a transaction server.

37. The universal-signature-object viewer of claim 29 further comprising:

a printing means for providing a print copy of information concerning the universal signature object.

38. The universal-signature-object viewer of claim 37 wherein the information concerning the universal signature object comprises at least one data field selected from the group of data fields comprising:

use-permission regarding permitted use of the universal signature object;
a list of items contained within the universal signature object;
at least one version of the digital data;
a digital signature;
a name of a signatory of the digital signature;
a timestamp of the digital signature; and
digital signature verification results.

39. The universal-signature-object viewer of claim 37 wherein the print means digitally watermarks the print copy.

40. The universal-signature-object viewer of claim 29 wherein:

the universal signature object further comprises at least one additional digital signature;
the digital signatures are timestamped; and
the viewer means displays the digital signature in timestamp order.

41. The universal-signature-object viewer of claim 29 wherein the universal-signature-object viewer operates within a browser application.

42. The universal-signature-object viewer of claim 29 wherein the universal-signature-object viewer is incorporated into the universal signature object.

43. The universal-signature-object viewer of claim 42 wherein the universal signature object is a standalone application.

44. The universal-signature-object viewer of claim 29 wherein the universal-signature-object viewer is a network application accessible via a network connection.

45. A method for digitally signing digital data, comprising:

accessing a signatory's private-public key pair;

authenticating the private-public key pair; and

in response to a universal signature object of the digital data not existing:

using the signatory's private key to generate a digital signature of signature data, wherein the signature data is a function of the digital data; and

generating the universal signature object of the digital data, the universal signature object comprising:

at least one version of the digital data, wherein each version has a file format;

the digital signature; and

information concerning an application compatible with the file format of at least one of the versions.

46. The method of claim 45 wherein the signature data is selected from the group comprising:

one of the versions of the digital data;

the universal signature object, prior to inclusion of the digital signature;

a hash of one of the versions of the digital data; and

a hash of the universal signature object, prior to inclusion of the digital signature.

47. The method of claim 45 wherein the universal signature object further comprises:

a timestamp of the digital signature.

48. The method of claim 47 wherein the signatory verifies the authenticity of the private-public key pair and provides the timestamp.

49. The method of claim 45 further comprising the steps of:

requesting a tracking number from a transaction server; and

transmitting at least a copy of the digital signature to the transaction server.

50. The method of claim 45 wherein at least one of the versions of the digital data has a non-native file format.

51. The method of claim 45 wherein the universal signature object further comprises:

the signatory's public key.

52. The method of claim 45 wherein the universal signature object further comprises:

use-permission information regarding the use of the universal signature object.

53. The method of claim 45 wherein the universal signature object further comprises: